

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



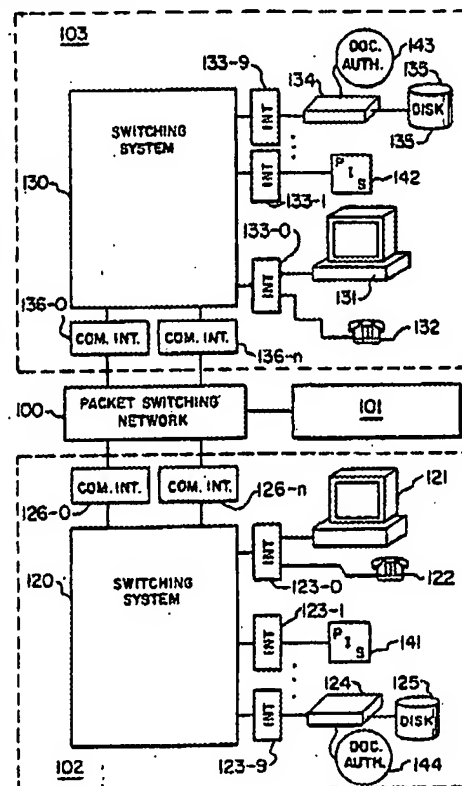
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04L 9/32		(11) International Publication Number: WO 92/09161
A1		(43) International Publication Date: 29 May 1992 (29.05.92)
(21) International Application Number: PCT/US91/08545 (22) International Filing Date: 15 November 1991 (15.11.91) (30) Priority data: 615,029 16 November 1990 (16.11.90) US (71)(72) Applicants and Inventors: DZIEWIT, Halina, S. [US/US]; 5260 Centennial Trail, Boulder, CO 80302 (US). GRAZIANO, James, M. [US/US]; 4662 Weld County Road 34, Platteville, CO 80651 (US). (74) Agent: GRAZIANO, James, M.; Dorr, Carson, Sloan & Peterson, 3010 East 6th Avenue, Denver, CO 80206 (US).		(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent). Published <i>With international search report.</i>

(54) Title: **KNOWLEDGE BASED SYSTEM FOR DOCUMENT AUTHENTICATION**

(57) Abstract

The document authentication apparatus provides document authentication and authenticity capability. Document authentication requires that the person to be charged apply an authenticating mark on the document indicating intent to authenticate the document. This requirement is analogous to a signature on a printed document and is implemented in the document authentication apparatus electronically through the use of both hardware and software. A program (143) which immediately checks the identicalness of the document at the transmitting (121) and receiving (131) station through a high speed comparison, locks in the document such that no modification can occur and then awaits authentication handshakes from the two end points. Such authentication is real-time and can be both hardware and software executable, i.e., password and physical confirmation.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LJ	Liechtenstein	SU ⁺	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LJ	Luxembourg	TG	Togo
DE*	Germany	MC	Monaco	US	United States of America
DK	Denmark				

⁺ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

1

**KNOWLEDGE BASED SYSTEM FOR
DOCUMENT AUTHENTICATION**

FIELD OF THE INVENTION

This invention relates to computer systems and, in particular, to apparatus for providing a document authentication and authenticity capability for the computer system, to produce an electronic document which satisfies the legal requirements for contracting as applied to printed documents.

PROBLEM

It is a problem in the field of computer systems to produce an electronic document that satisfies all the legal requirements associated with printed documents. Despite the availability of high technology in the field of electronic communication and record keeping, the business world almost exclusively relies on the generation and exchange of paper to consummate business transactions and to run day to day business operations. The predicted paperless office has failed to become a complete realization due to the difficulty in satisfying several significant legal issues with respect to electronic contracting: the requirement of a writing, the need for authenticating signatures that indicate the terms and conditions of an agreement are truly acceptable to both parties, and the question of document authenticity.

In a typical business transaction, two parties meet with the intent to reach an agreement with respect to the sale of merchandise. The parties exchange verbal understandings. At some point these

-2-

verbal understandings are put down on paper through the use of a word processor. A first draft is generated. The draft is sent by the vendor to the buyer. The buyer revises this draft copy and sends it back to the vendor. This process generally takes several iterations between the parties before a final written contract is approved and executed to consummate the deal. The contracting parties may take advantage of a computerized word processor that electronically retains the document on magnetic media (tape, disk) to allow easy retrieval, modification, transmission and storage. Document transmission between parties can be accomplished by teletype/facsimile and overnight mail. Alternatively, the majority of large corporations operate an electronic mailing system allowing them to relay documents to branch offices free from the postal system's constraints. Additionally, teleconferencing allows geographically separated people to conduct a group conference without travel. In this way, compromises and solutions may be agreed upon in real time.

Despite the availability of these technological advances, there remains a paper proliferation. Paper copies still serve as the standard and accepted way of contracting. Why the dependency on paper? Perception. The nature of electronic expressions raise issues of security, tangibility, reliability, authentication, longevity and validity. There is presently no electronic system that provides all of the safeguards and satisfies all of the legal requirements associated with paper documents. Therefore, electronic contracting has not been a viable alternative to paper documents.

-3-

SOLUTION

The above described problems are solved and a technical advance achieved in the field by the present document authentication and authenticity apparatus. This apparatus produces a final authenticated document using computerized techniques, which document satisfies the legal document authentication and authenticity requirements traditionally associated with printed documents. In addition, this apparatus eliminates many of the problems spawned by execution of paper contracts and the use of the postal service, such as the "battle of the forms" and the "mailbox rule".

The document authentication apparatus offers a number of hardware/software architectural options to provide document authentication and authenticity capability. Document authentication requires that the person to be charged apply an authenticating mark on the document indicating intent to authenticate the document. This requirement is analogous to a signature on a printed document and is implemented in the document authentication apparatus electronically through the use of both hardware and software.

The document authentication process is activated as part of a program which verifies the identicalness of the document at the transmitting and receiving station through a high speed comparison, locks in the document such that no modification can occur and then awaits authentication handshakes from the two end points. Once the identities of the signatories of the document are verified, the document authentication apparatus prompts the parties to authenticate the document by appending an electronic signature thereto. The actual "signing" or authenticating of the

-4-

electronic document can be implemented as an additional password step utilizing personnel identity validation apparatus. Therefore, two levels of password protection can be used such that there exists a separate "document authenticating password". Obviously, the more sophisticated the system, the more assured the court will be that the document authentication is valid.

The authentication of the document by the contracting parties consummates the execution of the document. The document authentication apparatus responds to the authentication operation by providing sufficient safeguards to insure that the contents of the file have not been modified or altered following the consummation of the contract without the alteration being detectable. This is typically accomplished by the generation of a "digital signature" that "fingerprints" the document such that not even a single bit of the document can be altered without this change being reflected in the digital signature. The authenticated document with the digital signature appended thereto can then be electronically archived on electronic media as a permanent document.

In this manner, no paper document version of this electronic contract need be produced. All the traditional elements of a paper contract are present in electronic form in the computer system. Each of these elements satisfy the traditional legal requirements for paper contracts, thereby implementing an electronic contract.

Additional capabilities are obtained since this is a knowledge based computer system and can automate much of the document creation and authentication

-5-

process. In particular, the creation of a multi party document, such as a contract, entails a significant amount of interaction among the contracting parties. Much of the interaction and energies of the parties are devoted to reviewing proposed variations in the terminology contained in the document and in reviewing the document to note all changes therein. In addition, the authentication process requires the physical exchange of the entire document among the parties so that each party can seriatim apply their signature to the document and finally receive an original signed by all the parties. The logistics of such a process can be complicated and are usually time consuming. The knowledge based system of the present invention can automatically compare two versions of the document to highlight any counterproposals therein. Furthermore, the system can review its internal rule set to determine whether these modifications are acceptable, in that the changes fall within acceptable predetermined limits. Once acceptance has been noted, the system can then automatically authenticate the document independent of human intervention. This is especially efficient in the arena of Electronic Document Interchange (EDI), where standard form messages are exchanged between the parties to order and invoice goods. These messages do not presently constitute a contract since there is no authentication of an agreed upon document. However, the present apparatus automatically authenticates the document in the EDI environment by using the original EDI order as the document and requesting that the essential data elements of the order, with optional additional recipient identification data, be echoed back to the transmitting party to signify acceptance

-6-

of the offer as embodied in the EDI order. The identicalness of the echoed terms and conditions to those originally transmitted is determined by the system of the present invention and, if a match occurs, the apparatus authenticates the document to create a binding contract between the parties.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 illustrates, in block diagram form, the structure of a multi-processor environment in which the document authentication apparatus is installed on one or more of the processors;

Figure 2 illustrates, in block diagram form, the structure of a typical document authentication apparatus;

Figures 3 to 5 illustrate, in flow diagram form, the operational steps of a document authentication process ;

Figure 6 illustrates, in flow diagram form, the specifics of the EDI contracting process.

-8-

DETAILED DESCRIPTION

The present document authentication apparatus produces a final authenticated document using computerized techniques, which document satisfies the legal document authentication and authenticity requirements traditionally associated with printed documents. In addition, this apparatus eliminates many of the problems spawned by execution of paper contracts and the use of the postal service, such as the "battle of the forms" and the "mailbox rule".

The document authentication apparatus offers a number of hardware/software architectural options to provide document authentication and authenticity capability. Document authentication requires that the person to be charged apply an authenticating mark on the document indicating intent to authenticate the document. This requirement is analogous to a signature on a printed document and is implemented in the document authentication apparatus electronically through the use of both hardware and software. The actual "signing" or authenticating of the electronic document can be implemented as an additional password step utilizing personnel identity validation apparatus. Therefore, two levels of password protection can be used such that there exists a separate "document authenticating password."

A program which immediately checks the identicalness of the document at the transmitting and receiving station through a high speed comparison, locks in the document such that no modification can occur and then awaits authentication handshake from the two end points. Such authentication is real-time and can be both hardware and software executable, i.e., password and physical confirmation. Obviously,

-9-

the more sophisticated the system, the more assured the court will be that the document authentication is valid, and that the contents of the file have not been modified or altered following the consummation of the contract without the alteration being detectable.

Additional capabilities are obtained since this is a knowledge based computer system and can automate much of the document creation and authentication process. In particular, the creation of a multi party document, such as a contract, entails a significant amount of interaction among the contracting parties. Much of the interaction and energies of the parties are devoted to reviewing proposed variations in the terminology contained in the document and in reviewing the document to note all changes therein. In addition, the authentication process requires the physical exchange of the entire document among the parties so that each party can seriatim apply their signature to the document and finally receive an original signed by all the parties. The logistics of such a process can be complicated and are usually time consuming. The knowledge based system of the present invention can automatically compare two versions of the document to highlight any counterproposals contained therein. Furthermore, the system can review its internal rule set to determine whether these modifications are acceptable, in that they fall within predetermined acceptable limits. Once acceptance has been noted, the system can then automatically authenticate the document, independent of human intervention. This is especially efficient in the arena of Electronic Document Interchange (EDI), where standard form messages are exchanged between the parties to order and invoice goods. These messages do

-10-

not presently constitute a contract since there is no authentication of an agreed upon document. However, the present apparatus automatically authenticates the document in the EDI environment by using the original EDI order as the document and requesting that the essential data elements of the order, with optional additional recipient identification data, be echoed back to the transmitting party to signify acceptance of the offer as embodied in the EDI order. The identicalness of the echoed terms and conditions to those originally transmitted is determined by the system of the present invention and, if a match occurs, the apparatus authenticates the document to create a binding contract between the parties.

Requirement of a Writing

The legal requirements for a contract have their origins in the traditional paper methods of business transactions. One of these key legal requirements is the Statute of Frauds. Under the Statute of Frauds, if the contract takes longer than one year to perform or involves a monetary sum greater than \$500, it must be in writing. The writing must specify all the terms and conditions of the contract. Mutual assent to these terms and conditions must be demonstrated by an authenticating mark, typically the signature of both parties. The rationale behind the Statute of Frauds is to provide a writing which will afford a basis for believing that the oral evidence offered rests on a real transaction and to ensure the valid existence of a contract. Thus, a writing is required to provide evidence of a valid agreement between the parties.

The writing requirement of the Statute of Frauds can be satisfied by handwritten or typewritten

-11-

versions of a document or by telegram. A telegram is generated as electrical signals transmitted over electrical conductors or microwave transmissions. A transmission which generates a telegram is clearly an intangible method of exchanging information to produce a human readable document - a printout. A computer transmission is another intangible method of exchanging information to produce a human readable document. Both the telegram and computer methods of contracting should satisfy the Statute of Frauds in that both transmissions can be reduced to a human readable document.

The computer media on which an electronic contract is stored as data also provides a permanent record to which a court can turn in the event of a dispute. The lifetime of computer media and the state of the art in storing this media not only ensures the existence of a representation of the parties' understanding, but endures beyond the lifetime of paper. Should the contents of an electronic contract be brought into question, the data comprising the terms and conditions of the electronic contract is immediately retrievable and transformable to a human readable document.

Requirement of an Authenticating Signature

Another requirement issue which becomes evident under the Statute of Frauds in regard to the use of electronic contracts is the signature requirement by the person to be charged. The Uniform Commercial Code (UCC) defines "signed" to include "any symbol executed or adopted by a party with present intention to authenticate a writing." The term "authentication" is included to "make it clear that a complete handwritten

-12-

signature is not required." A signature appended to a contract must establish an "evidentiary connection to the signatory." As discussed subsequently, the state of the art does not preclude the ability to authenticate in the context of electronic contracting. Additionally, the present laws may be interpreted to encompass state of the art authenticating methods.

American Jurisprudence on the Statute of Frauds states that:

the signature must be made or adopted with the declared or apparent intent of authenticating the writing relied upon as a memorandum, and not by way of mere recital or identification. Especially if the signature is affixed by means other than the hand of the signer,...it is essential that the act be done with intent to authenticate the instrument.

Document Authenticity

In the above analysis, every issue presented rests upon the credibility of the computer data that represents the contract. The viability of such a contract requires strict adherence to an ordered data file security procedure. These document authenticity safeguards must ensure that the document has not been altered since unauthorized modifications to computer media expressions are not easily detectable. Therefore, to satisfy the document authenticity requirement of identical terms and conditions, the generally accepted criteria of a locked file cabinet, valid signature, file security and acceptable mode of "sending" the contract must be met. The computer and its peripheral equipment must ensure the presence of the above-identified four factors.

The equivalent to the paper requirements must be first, the locked file cabinet demonstrated in the

-13-

computer environment of files stored on the computer disk. Second, the equivalent of traditional "signing" must be demonstrated. Third, a clear demonstration that no unauthorized modifications were made to the computer expressions. Finally, electrical representations must follow the same transmission security requirements ascribed to traditional contracts transmitted by mail. The following description indicates some of the elements provided in the present document authentication system to satisfy each of these requirements.

Document Access

The first step in ensuring proper document authenticity, as a minimum requirement, simple physical restrictive access to the computer should be implemented. In other words, by simply locking the doors to the computer system and its associated terminals, a modest security procedure is in place. Computer access can be achieved via telephone lines by any average computer hacker. Therefore, a variety of hardware and software methods exist to ensure that the locked file cabinet equivalent exists. For example, a callback modem can provide additional security from intruders. This device responds to a person calling the computer by requesting that the person identify themselves. The computer then disconnects from the call and telephones the identified caller at a predesignated telephone number stored in the computer memory and associated with the identified caller. This type of security arrangement, although more sophisticated than a locked room, is still subject to circumvention. Therefore, the state of the art offers still more sophisticated methods of preventing access,

-14-

and, in particular, access to the computer files.

Passwords are typically used to validate the identity of the user. The software operating the computer prompts the user to enter a password that is theoretically known only to the user before access to the computer's files is granted. Therefore, access is password protected such that only a single user may gain entry. The accuracy of user identity validation can be improved by the addition of various peripheral devices that measure some immutable physical characteristic of the user. These devices include fingerprint scanners, voiceprint identifiers, retina scanners, etc. Each of these devices can be preprogrammed to respond to only the authorized user and operate with a high level of confidence. Clearly, sophisticated hardware and software methods exist to secure access to computer files, i.e., the locked cabinet analogy.

Document Authentication

The state of the art also offers hardware/software architectural options to provide document authentication capability. Document authentication requires that the person to be charged apply an authenticating mark on the document indicating intent to authenticate the document. This analogy to the signature is also electronically viable through the use of hardware and software. The actual "signing" or authenticating of the electronic document should be implemented as an additional step utilizing the above described technology. Therefore, two levels of password protection can be used such that there exists a separate "document authenticating password."

A program which immediately checks the

-15-

identicalness of the document at the transmitting and receiving station through a high speed comparison, locks in the document such that no modification can occur and then awaits authentication handshake from the two end points. Such authentication is real-time and can be both hardware and software executable, i.e., password and physical confirmation. Obviously, the more sophisticated the system, the more assured the court will be that the document authentication is valid, and that the contents of the file have not been modified or altered following the consummation of the contract without the alteration being detectable.

Document Authenticity

One method of ensuring document authenticity is the use of a "digital signature." Computer software which employs a complex mathematical formula produces a series of 0 and 1 bits that are appended to the file to uniquely identify the contents of the file. This is accomplished by the use of a "hashing routine" that uses each character in the file in a complicated mathematical computation to obtain, for example, a 128 character digital signature. Thus, the digital signature is dependent on the contents of the file and if even a single bit of the file is changed, the digital signature does not match. If a single character of the file is changed, then approximately 50% of the characters in the digital signature will change. The probability of two documents having the same digital signature using this procedure is less than one in 1,000 trillion. This adequately ensures that the contents of the original contract cannot be altered without the modification being detectable.

-16-

File Transmission

Alterations of the contract during transmission is particularly a concern with respect to written and electronic contracts. The written document can easily pass through human hands that can expertly alter the contents of the paper expression. Detecting a switch in paper documents is nearly impossible. Electronic document transmission is clearly superior to paper documents in that sophisticated technology not only allows for secure transmissions, but offers technology to detect any tampering. If security is not a factor and the document is sent via common carrier telecommunication facilities, the transmission is sent concurrently with many other transmissions. Anyone can access these transmissions, but finding a specific transmission and associating it with a particular sender is difficult considering the number of communication channels supported by one common carrier facility. Physical "wiretapping" requires access to a user's facilities, and thus, is equally prohibitive if adequate on site security measures are employed.

An additional level of security is obtained by the use of encryption, where the entire document is translated into coded form using a secret cipher key. This protects the document from being read by third parties, but does not protect sender and receiver from fraud committed by each other, since both have knowledge of the cipher key. More complex encryption systems that use a third party trustee are available, but are costly to implement. Therefore, technology exists which serve to secure transmissions and permit authentication of agreed upon terms and conditions. The National Bureau of Standards has adopted an encryption algorithm known as the Data Encryption

-17-

Standard (DES). This encryption key uses 64 bits and therefore does not require much processing time or assume much storage space. Additionally, the associated software is relatively inexpensive. A more secure and complex system that minimizes the possibility of fraud by the contracting parties is the RSA Public Key Cryptosystem. This system uses two encryption keys. A "private key" is used by the document sender to scramble the data while a "public key", known to the document recipient, is used to decode the received document. Since the registered public key will unscramble only data that was scrambled with the private key, the parties can identify each other. This system is analogous to handwritten signatures in that the electronic signature can be verified but not easily forged. This system can be used in lieu of the above described DES system where the trustworthiness of the other party is in doubt.

System Architecture

The document authentication apparatus is typically installed as part of a computer system, either a personal computer or a minicomputer. The apparatus illustrated in Figure 1 represents the interconnection of a plurality of processors, each of which is associated with one of the parties to a contract negotiation, and one or more of which processors are equipped with the document authentication apparatus. These parties can be geographically separated, such as in different parts of the country, or can be within the same building.

A typical system installation 102 can be processor 124, equipped with disk memory 125,

-18-

personnel identification apparatus 141 and one or more terminals 121. The party at terminal 121 is also equipped with a telephone 122 for voice communication with the other parties to the contract negotiation. A communication interface 123-0 is provided to interconnect terminal 121 and telephone 122 via voice/data interface 123-0 and leads 127-0. In addition, switching system 120 interconnects via trunk circuits 126-0 to 126-n to the common carrier communication facilities, represented in Figure 1 as packet switching network 100. The switching system 120 can be a telephone switching system that establishes voice communication connections from telephone station set 122 and data communication connections from terminal 121 and processor 124 to packet switching system 100. In many existing telephone switching systems, the voice and data communication connections are established independent of each other via distinct communication paths. In addition, processor 124 is equipped with document authentication software 144 that is described in detail below. The document authentication software 144 provides control of the documentation authentication process and provides all the elements necessary to satisfy the legal requirements of a contract.

Another alternative typical system installation 103 can be processor 134, equipped with disk memory 135 and personnel identification apparatus 142. Processor 134 is also equipped with document authentication software 143 that is described in detail below. The document authentication software 143 provides control of the documentation authentication process and provides all the elements

-19-

necessary to satisfy the legal requirements of a contract. In addition, one or more personal computers 131 provide distributed processing capability. The user at personal computer 131 is also equipped with a telephone 132 for voice communication with the other parties to the contract negotiation. A voice/data communication interface 133-0 is provided to interconnect personal computer 131 and telephone 132 with switching system 130. In addition, switching system 130 is connected via trunk circuits 136-0 to 136-n with the common carrier communication facilities, represented in Figure 1 as packet switching network 100. The switching system 130 can be a telephone switching system that establishes voice communication connections from telephone station set 132 and data communication connections from processor 134 and personal computer 131 to packet switching system 100. In state of the art telephone switching systems, the voice and data communication connections are established as a single combined communication connection. The present such combined communication connections are referred to as Integrated Services Digital Network (ISDN) connections. The ISDN communication methodology provides a combined voice/data communication path that integrates telephone station set 132 with personal computer 131 to enable the user to have the full spectrum of communication capability with the other parties via a single interface and communication connection.

The final computer system 101 illustrated as a block in Figure 1 and parallels the structure of system installation 102 or 103 and is illustrated for the purpose of discussing three party contracts and /or the use of a third-party trustee as is described

-20-

in further detail below.

Documentation Authentication Software

The document authentication software, such as 143, is illustrated in further detail in Figure 2. This software includes document authentication control element 201 which serves as the basic program control block. Various subroutines (202-207) are connected to document authentication control 201 to provide the specialized features and hardware control elements. File lock element 202 controls access to the document or file such that only the contracting parties can access the document. Access to the document is rigorously controlled to prevent tampering with the document contents during editing and execution. Communication control element 203 manages all communication among the processors to limit the possibility of unauthorized users from accessing the document. Encryption/decryption element 204 provides the capability to encode and decode the document for transmission over the packet switching network 100 to prevent interception of the document contents during the transfer of the document among the parties. The personnel identification sensor scanner element 205 provides control over the parties identification verification process. Digital signature generator element 206 produces a digital signature that is appended to the final signed document to prevent the contents of the document from being altered without detection. The digital signature thereby supplies document content validation for archival purposes. The file archive element 207 relocates the executed document to a secure data storage media location for long term archival purposes. This element also

-21-

manages the file lock and access control software that prevents unauthorized or inadvertent file access.

Document Authentication Process

In order to more fully understand the operation of the document authentication apparatus, the process of authenticating a document is described in flow diagram form in Figures 3 to 5, with reference to the hardware and software elements of Figures 1 and 2. In this process it is assumed for the purpose of discussion, that a user at system installation 102 and a user at system installation 103 are the two parties to a contract for the purchase of goods. These two parties are not colocated and for description purposes are assumed to be located in Seattle, Washington and Omaha, Nebraska, respectively. The two parties are linked by the common carrier facilities 100 available to the public, such that both voice and data communications are concurrently carried via these common carrier facilities 100 between the two parties. For simplicity of description, it is assumed that the document or contract of interest to the two parties resides on processor 134 although copies of this document can also be stored on personal computer 131 and processor 124.

Document Editing

The document editing process typically begins with a user (first party) logging on to processor 134 and accessing a file. This is accomplished at step 301 by first party at personal computer 131, for example, unlocking the personal computer 131 with a key as is found on the IBM personal computers. First party then establishes a data communication connection

-22-

via voice/data interface 133-0, switching system 130, voice/data interface 133-9 to processor 134. Once connected to processor 134, first party logs into the processor 134 at step 301 by providing a user identification password in response to a prompt from processor 134. This password should be known only to first party and uniquely identifies first party to processor 134, thereby preventing unauthorized parties or other users from accessing first party's files resident on processor 134. At step 302, first party requests access to a file named "contract" for the purpose of editing this file. If this file is stored in cache memory of processor 134, it is immediately transmitted to and displayed on the screen of personal computer 131. If the file is archived in disk memory 135 at step 303, processor 134 requests file "contract" from disk memory 135 that serves processor 134. In response to such a request, disk memory 135 transfers file "contract" to processor 134 which transmits file "contract" via switching system 130 to personal computer 131, where the file is displayed for first party to edit.

If first party elects to unilaterally edit the file "contract", this is accomplished in well known fashion at step 304. The edited file can be saved at step 305 and editing terminated. Alternatively, at this juncture, or even at step 304, first party can request the addition of the other contracting party (second party) who is a user on processor 124. This is accomplished by first party requesting access to the document authentication software 143 resident on computer 134 at step 306. Document authentication software 143 interfaces with first party via document authentication control 201 which provides a user

-23-

friendly interface to enable a user to step through the document authentication process.

File Lock

Document authentication control 201 at step 307 produces a user prompt/query or a menu to enable first party to signify the requested action. For example, first party at step 308 designates file "contract" as the document of interest. Document authentication control 201 activates subroutine file lock 202 which loads file "contract" into the document authentication software 143 and prevents uncontrolled access or modification of this file. At this stage, the file can be edited by preauthorized users (the contracting parties): first and second parties.

Communication Control

Once the file "contract" is loaded, first party, in response to a query from document authentication control 201, requests that a communication connection be established to second party. Document authentication control 201 activates communication control 203 to establish voice and data communication connections to second party. This is accomplished by communication control 203 at step 309 either querying first party or accessing a predetermined list of contracting parties to obtain the identification of the contracting parties for the file "contract". At step 310, communication control 203 establishes data communication connection via communication interface 133-9, switching system 130, communication interface 136-0, packet switching system 100, communication interface 126-0, switching system 120, communication interface 123-0 to processor 124 and terminal 121.

-24-

Concurrently, switching system 130 may establish a voice communication connection from telephone station set 132, voice/data communication interface 133-0, switching system 130, communication interface 136-0, packet switching system 100, communication interface 126-0, switching system 120, voice/data communication interface 127-0 to telephone station set 122. The second party at terminal 121 can access file "contract" as if it were resident on processor 120 and can simultaneously discuss the contents of file "contract" via telephone station set 122. Thus, both first party and second party concurrently view the same document on their respective terminals 131, 121 and can exchange verbal communication via their respective telephone station sets 132, 122. In this fashion, the contract can be edited in real time and a more timely resolution of differences reached.

Alternatively, second party at terminal 121 can be connected on a data communication connection via voice/data communication interface 123-0, switching system 120, data communication interface 123-9, processor 124, data communication interface 123-9, switching system 120, communication interface 126-0 to packet switching system 100. The exact details of the voice and data communication connections are a function of the implementation details of the switching systems and the computer equipment used.

Additional parties can be added seriatim to this voice/data communication connection if a plurality of contracting parties are required. This is accomplished at step 311 by the step of determining whether all the requested parties, as described in the preassigned list or as entered by first party, have been connected together. If all parties are not yet

-25-

connected, processing returns to step 310 where another communication connection is established. For the purposes of simplicity, only a two party connection is described herein. Communication control 203 therefore views the communication connections as the interconnection of first party at one of the communication lines of switching system 130 with at least one other contracting party connected to corresponding ones of communication interfaces 136-0 to 136-n that interconnect these other contracting parties with system installation 103 via packet switching system 100.

Editing of the file "contract" can now be accomplished by the plurality of contracting parties in real time at step 312. All the contracting parties (first and second) have editing capability via their respective terminals 131, 121 and voice communication capability via their respective telephone station sets 132, 122. If the parties agree to store and not authenticate this file, at step 313 document authentication control 201 proceeds to store and lock the file "contract". This is controlled by file lock software 202 which disconnects the parties from the communication connections and proceeds to store and lock the file "contract" in memory such as disk drive 135.

If any of the parties connected to system installation 103 via communication control 203 elect to authenticate the file "contract", at step 314 document authentication control 201 activates file lock software 202 to place the file "contract" in a read-only mode for authentication purposes to prevent any further changes to this file by any of the contracting parties, to thereby avoid tampering. At

-26-

step 315, document authentication control 201 queries all the parties to determine whether distributed review of the file "contract" is desired. If not, the authentication process continues at step 321 where the personnel identification process is initiated. However, if distributed review is requested, the document authentication control 201 at step 316 enters the encryption session of encryption/decryption software 204.

Encryption/Decryption of the File Contents

At step 316, encryption/decryption software 204 encrypts the file "contract" using one of the well-known processes described above, such as the Data Encryption Standard. At step 317, encryption/decryption software 204 requests communication control 203 to transmit the encrypted file to all the parties via the existing communication connections. Once the encrypted file has been received by the parties, each party can use decryption software, resident on their respective processors 124, 134, to decrypt the received encrypted file at step 318. The processors 124, 134 can then at step 319 compare the decrypted file to their copy of the file as recorded in their "own copy" version to insure that no discrepancies exist in the file "contract" as presently stored in the locked file form in document authentication software 143. At step 320, each user can elect to exit from the authentication process or continue with the formalization of the file "contract". An alternative to distributing the file to all the contracting parties is for document authentication software 143 to compare the copy of the file stored on processor 124 with the copy of the file

-27-

stored on processor 134 for identicalness. Then, at step 316, processor 124 encrypts the version of file "contract" that is stored on processor 124 and transmits the encrypted file at step 317 to processor 134 over the above-described data communication connection. The recipient party at processor 134 is document authentication software 143 which decrypts the received encrypted file and at step 319 compares the received decrypted file with the version stored on processor 134. If the two versions of the file "contract" match, at step 320, the document authentication process continues as noted above.

Personnel Identification Sensors

The personnel identification process is initiated at step 321 by all the authenticating parties assenting to the form and content of the file "contract" as is presently stored in the document authentication software 143. The assent is obtained by personnel identification process 205 polling all the parties seriatim to obtain their initial confirmation that authentication is appropriate. At step 322, personnel identification process 205 enables and scans a sensor (ex. device 142) associated with one of the contracting parties. The sensors, as described above, can be as elemental as a prompt to the terminal associated with the selected party to enter a password that is theoretically known only to the selected party. The accuracy of personnel identity validation can be improved by the addition of various peripheral devices 142, 141 that measure some immutable physical characteristic of the party. These devices include fingerprint scanners, voiceprint identifiers, retina scanners, etc. Each of these

-28-

devices can be preprogrammed to respond to only the authorized party and operate with a high level of confidence. Therefore, the personnel identification process 205 can signal a peripheral device 142 that is colocated with the selected party's terminal 131 to obtain data therefrom indicative of some selected immutable physical characteristic of the selected party. At step 323, personnel identification process 205 compares the data received from the selected sensor 142 with data stored in its memory indicative of the correct party identification. Some sensors 142 themselves include preprogrammed data that performs the comparison test and outputs a confirmation or a denial of the party's identification. At step 324, if there is not a match, processing is aborted and an error condition is reported to all parties. If a validation is determined at step 324, then the next party in the process is confirmed until all the parties are determined at step 325 to have been validated. Once validation of the identification of all the contracting parties is obtained, then the file "contract" is "signed" by all the parties and the legal document has been executed electronically.

Digital Signature Generator

In order to insure the credibility of the executed file "contract", document authentication software 143 can append a digital signature to the executed file to prevent undetected unauthorized tampering with the contents of the file "contract". This is accomplished at step 326 by document authentication control 202 activating digital signature generator 206 to produce a digital signature based on the contents of file "contract". The digital

-29-

signature can be generated by either hardware or software, depending upon the particular process selected. The digital signature is typically generated by computer software which employs a complex mathematical formula to produce a series of 0 and 1 bits that are appended to the file to uniquely identify the contents of the file. This is accomplished by the use of a "hashing routine" that uses each character in the file in a complicated mathematical computation to obtain, for example, a 128 character digital signature. Thus, the digital signature is dependent on the contents of the file and if even a single bit of the file is changed, the digital signature does not match. If a single character of the file is changed, then approximately 50% of the characters in the digital signature will change. The probability of two documents having the same digital signature using this procedure is less than one in 1,000 trillion. This adequately ensures that the contents of the original contract cannot be altered without the modification being detectable.

File Archival

Once the digital signature is produced, document authentication control 201 transfers the authenticated file and its associated appended digital signature to file archive process 207. At step 327, file archive process 207 stores the file in memory, such as disk memory 135. In addition, if so requested, copies of the file are transmitted at step 328 to all the contracting parties to provide each party with an executed digitally signed copy of the file "contract". The transmission can include encryption as described above. At this juncture, the contract has been

-30-

reviewed by all parties, "signed" by all parties using special authentication processes, and "sealed" by use of a digital signature. For security purposes, the standard business practice of storing multiple copies can be used by any or all of the contracting parties. Thus, the electronic data can be stored on multiple disks or on a memory that provides a dual copy protection scheme. As can be seen from this description, no paper copy of the contract has been generated, nor needs to be produced.

Third Party Trustee

An alternative to the above-described process is the use of third party trustees. In this application, another party is added to the contract process for security reasons. The third party is a fiduciary, such as a bank, that has no proprietary or financial interest in the subject matter of the contract or any financial ties to any of the contracting parties. The third party, at system installation 101 (details not shown, but similar or identical to any of the party's computer systems) is the repository for the document authentication software and the file "contract". The third party controls the communication connections and can even provide facilities of their own at which the respective parties in Seattle and Omaha can visit to access terminals 121, 131 and personnel identification devices 141, 142 that are controlled by the third party. It is evident from the above description, that such a variation can be accomplished in straightforward fashion based upon the description provided herein.

-31-

Knowledge Based Document Authentication Control

The above-described apparatus provides document authentication capability for any multi-party or single party situation. Of particular interest is the EDI environment, where a first party transmits an electronic order to a second party. The transmission of this electronic order is typically handled by a common carrier local area network, which electronically deposits the order in the electronic mailbox of the second party recipient. The second party periodically retrieves the electronic messages deposited in this mailbox and acts on the messages retrieved therefrom. However, absent a return message to the first party, no contract is created. The failure of the second party to respond to and authenticate the first party's offer creates a situation where the essential elements of a contract as outlined above have not been satisfied. In order to create a contract, some acceptance of the first party's offer must be transmitted by the second party to the first party. This acceptance can be in any form, as long as it indicates acquiescence to the received offer. The document authentication apparatus includes a knowledge based system that enables this essential contract element to be implemented in automatic form. In particular, if the second party, on receipt of the first party's offer, transmits an electronic (ex. - EDI standard form) response to the first party signifying acceptance of the offer, an electronic contract is formed. This response can be an echoing of the basic terms of the first party's offer, along with an identification of the second party. The identification can include a password to validate the identity of the second party, but this is

-32-

not essential. The knowledge based system monitors all offers transmitted by the first party, and creates a library or listing of all outstanding offers. This list would typically include: the identity of the second party, quantity and price of goods, shipping date and other essential terms of the offer, such as expiration date of the offer. Upon receipt of this offer, second party transmits the data stored in the list, as obtained from the originally transmitted offer, to the first party along with data identifying the second party. The knowledge based system compares the received acceptance from the second party with the offer data stored in the list. If there is a match, the document authentication system notes this document as authenticated. The difference between this transaction and the human user based transaction described above, is that the basic working relationship between the parties is typically well-established and each offer and acceptance interchange simply represents another transaction in a long sequence of transactions under the umbrella of the underlying business relationship, which may be described in an underlying business relationship contract. Each subsidiary interchange is itself a contract, with reference to additional terms and conditions as enumerated in the business relationship contract. The subsidiary interchange does not require significant human involvement and the offer is created by a human, but its acceptance, and conformance checking with the offer can be performed by the document authentication system without the need for human intervention.

The failure of the acceptance to match the offer can be processed by the knowledge based system in a

-33-

number of ways. A simple response is to alert a human operator of the failure to match and expect manual correction of any discrepancy. Another capability of the knowledge based system is to determine whether the acceptance, or counteroffer - since it does not match the offer, falls within a predetermined range of variability. Thus, the knowledge based system contains a set of rules indicative of acceptable bounds on substantive contract terms. Therefore, when the counteroffer is received from the second party, the knowledge based system identifies the variation between the offer and counteroffer. This variation is then factored using the preprogrammed rule set in the document authentication system to determine whether the change in substantive offer terms is acceptable to the first party. If so, the counteroffer is accepted and authenticated, and the revised and acceptable terms transmitted to the second party as confirmation of the counteroffer. If not acceptable, the knowledge based system can itself use its embedded rule set to make a new offer to the second party and reinitiate the original offer process. Alternatively, the knowledge based system can request human intervention if the counteroffer varies in substantive terms from the offer by greater than a predetermined amount.

An example of this process is illustrated in flow diagram form in Figure 6. An offer of purchase of 10,000 machine screws at \$25.00/100 to be shipped in two weeks C.O.D. is transmitted by knowledge based system 210 of first party to second party at step 601. At step 602, these terms and conditions are written into a table of outstanding offers 211 contained within knowledge base system 210. At step 603, knowledge based system 210 receives from packet

-34-

switching network 100 a counteroffer transmitted by second party of 15,000 machine screws at \$24.50/100 to be shipped in three weeks C.O.D.. Knowledge based system 210 at step 604 strips the data from the counteroffer and at step 605 compares each segment of the counteroffer with the originally transmitted offer as stored in table 211. With each mismatch discovered in this comparison, knowledge based system 210 at step 606 compares the magnitude of the discrepancy with the permissible threshold for this item as stored in knowledge based system 210. As can be seen from the entries in table 211 in Figure 2, the quantity is permitted to vary by 20% and the counteroffer represents a 50% change from the offer. The remaining items in the counteroffer fall within the range of permitted values noted in table 211. Therefore, at step 607, the knowledge based system signifies failure to match terms and conditions. At step 608, knowledge based system 210 formulates and at step 609 transmits a new offer to the second party based upon the original offer and the received counteroffer. If a match had been determined, the counteroffer would be authenticated at step 610 and its terms merged into the original offer. As can be seen from this description, there are many possible comparison and new offer algorithms that can be used in this apparatus. A simplistic one is shown here for illustrative purposes and it is expected that more complex programs can be implemented, envisioning the repeated interchange of offers and counteroffers between the knowledge based systems of first and second parties. What is important to note here is that the basic comparison function is best handled by a knowledge based system rather than a human for

-35-

accuracy and economic reasons. Similarly, minor variations in contract terms do not require human intervention, especially in a trading partner situation where each subsidiary transaction represents one small interchange in a much larger business relationship and does not warrant excessive human scrutiny and intervention. Most importantly, the automatic document authentication process illustrated herein creates legally binding contracts, without the need for human intervention beyond the original offer, and possibly the creation of the acceptance or counteroffer. The knowledge based system can act as the agent of the first party and authenticate the contract.

While a preferred embodiment of the invention has been disclosed herein, it is expected that those skilled in the art can and will devise alternative arrangements that fall within the scope of the appended claims.

-36-

WE CLAIM:

1. In a data processing system that includes a processor (134), at least one data terminal (131) and at least one data communication port (136), a document authentication system comprising:

means (130, 133) for interconnecting a first user at a said data terminal (131) with said processor (134);

means (143), responsive to said first user transmitting a document origination signal from said data terminal (131) via said interconnecting means (130, 133) to said processor (134), for transmitting a document, identified by said document origination signal, from said processor (134) to a second user via said data communication port (136);

means (210), responsive to receipt of a document authentication signal from said second user, for comparing said received document authentication signal with said document to determine whether said received document authentication signal contains data that matches corresponding data in said document; and

means (201-207), responsive to said comparing means (210) determining a match between said received document authentication signal and said corresponding data in said document, for authenticating said document.

2. The system of claim 1 further comprising:

means (141, 142, 205), responsive to said second user inputting a document authentication signal, for validating the identity of said second user.

3. The system of said claim 2 wherein said validating means (141, 142, 205) comprises:

-37-

means (141) for measuring an immutable physical characteristic of said second user; and

means (205) for comparing said measured immutable physical characteristic with data, stored in a memory, indicative of said immutable physical characteristic of said second user as previously measured.

4. The system of claim 1 further comprising:

means (142, 205), responsive to said first user inputting a document origination signal, for validating the identity of said first user.

5. The system of said claim 4 wherein said validating means (142, 205) comprises:

means (142) for measuring an immutable physical characteristic of said first user; and

means (205) for comparing said measured immutable physical characteristic with data, stored in a memory, indicative of said immutable physical characteristic of said first user as previously measured.

6. The system of claim 1 further comprising:

means (206) for appending a digital signature to said authenticated document to detect any alteration of said authenticated document.

7. The system of claim 1 wherein said comparing means (210) includes:

means (602-605) for identifying differences between said data contained in said received document authentication signal and said corresponding data in said document;

means (211) for storing data indicative of a set of predetermined thresholds, each threshold in said

-38-

set of thresholds corresponding to a maximum allowable variation in one of said corresponding data in said document; and

means (607) for indicating a match between said received document authentication signal and said document when said identified differences do not exceed said maximum allowable variation for each of said corresponding data.

8. The system of claim 7 wherein further comprising:

means (612), responsive to said indicating means (607) failing to indicate a match, for producing an alert to denote a failure of said document authentication signal to match said document; and

means (610), responsive to said first user transmitting a document authentication signal to said processor (134) subsequent to said second user transmitting a document authentication signal to said processor (134), for authenticating said document inclusive of said identified differences contained in said second user document authentication signal.

9. The system of claim 8 further comprising:

means (608), responsive to at least one of said identified differences exceeding said maximum allowable variation for one of said corresponding data, for revising said document; and

means (609) for transmitting said revised document to said second user.

10. The system of claim 1 wherein said second user comprises a processor (124), programmed to respond to said document transmitted by said

-39-

transmitting means (143).

11. In a data processing system that includes a processor (134), at least one data terminal (131) and at least one data communication port (133), a method of document authentication comprising the steps of:

interconnecting a first user at a said data terminal (131) with said processor (134);

transmitting, in response to said first user transmitting a document origination signal from said data terminal (131) to said processor (134), a document, identified by said document origination signal, to a second user via said data communication port (133);

comparing, in response to receipt of a document authentication signal from said second user, said received document authentication signal with said document to determine whether said received document authentication signal contains data that matches corresponding data in said document; and

authenticating, in response to said step of comparing determining a match between said received document authentication signal and said corresponding data in said document, said document.

12. The method of claim 11 further comprising the step of:

validating, in response to said second user inputting a document authentication signal, the identity of said second user.

13. The method of claim 12 wherein said step of validating includes:

measuring an immutable physical characteristic of

-40-

said second user; and

comparing said measured characteristic with data, stored in a memory, indicative of said immutable physical characteristic of said second user as previously measured.

14. The method of claim 11 further comprising the step of:

validating, in response to said first user inputting a document origination signal, the identity of said first user.

15. The method of claim 14 wherein said step of validating includes:

measuring an immutable physical characteristic of said first user; and

comparing said measured characteristic with data, stored in a memory, indicative of said immutable physical characteristic of said first user as previously measured.

16. The method of claim 11 further comprising the step of:

appending a digital signature to said authenticated document to detect any alteration of said authenticated document.

17. The method of claim 11 wherein said step of comparing includes:

identifying differences between said data contained in said received document authentication signal and said corresponding data in said document;

storing data indicative of a set of predetermined thresholds, each threshold in said set of thresholds

-41-

corresponding to a maximum allowable variation in one of said corresponding data in said document; and

indicating a match between said received document authentication signal and said document when said identified differences do not exceed said maximum allowable variation for each of said corresponding data.

18. The method of claim 17 wherein further comprising the steps of:

producing, in response to said step of indicating failing to indicate a match, an alert to denote a failure of said document authentication signal to match said document; and

authenticating, in response to said first user transmitting a document authentication signal to said processor (134) subsequent to said second user transmitting a document authentication signal to said processor (134), said document inclusive of said identified differences contained in said second user document authentication signal.

19. The method of claim 18 further comprising the step of:

revising said document, in response to at least one of said identified differences exceeding said maximum allowable variation for one of said corresponding data; and

transmitting said revised document to said second user.

20. The system of claim 11 wherein said second user comprises a processor (124), programmed to respond to said transmitted document.

1/6

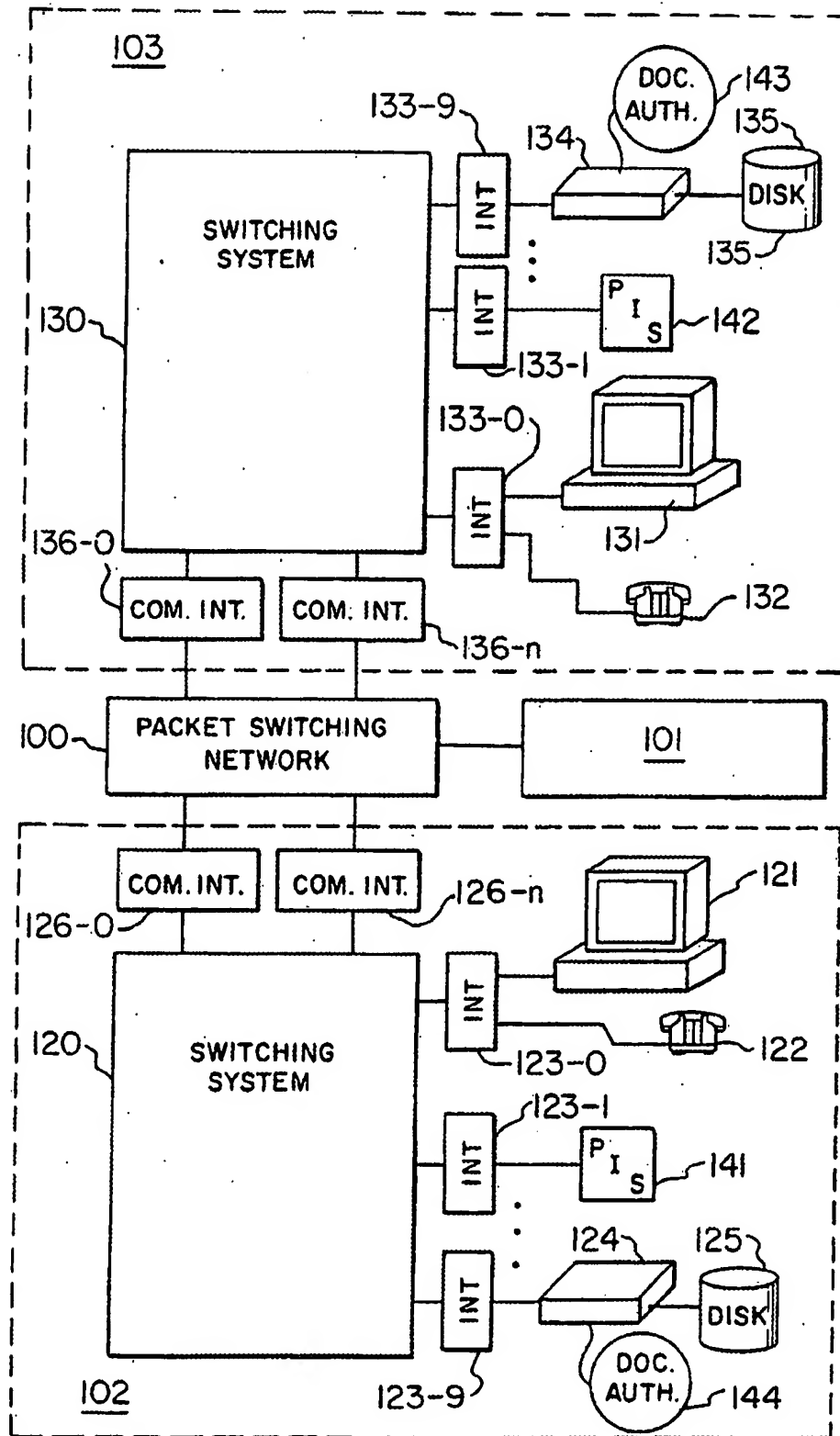


FIG. 1.

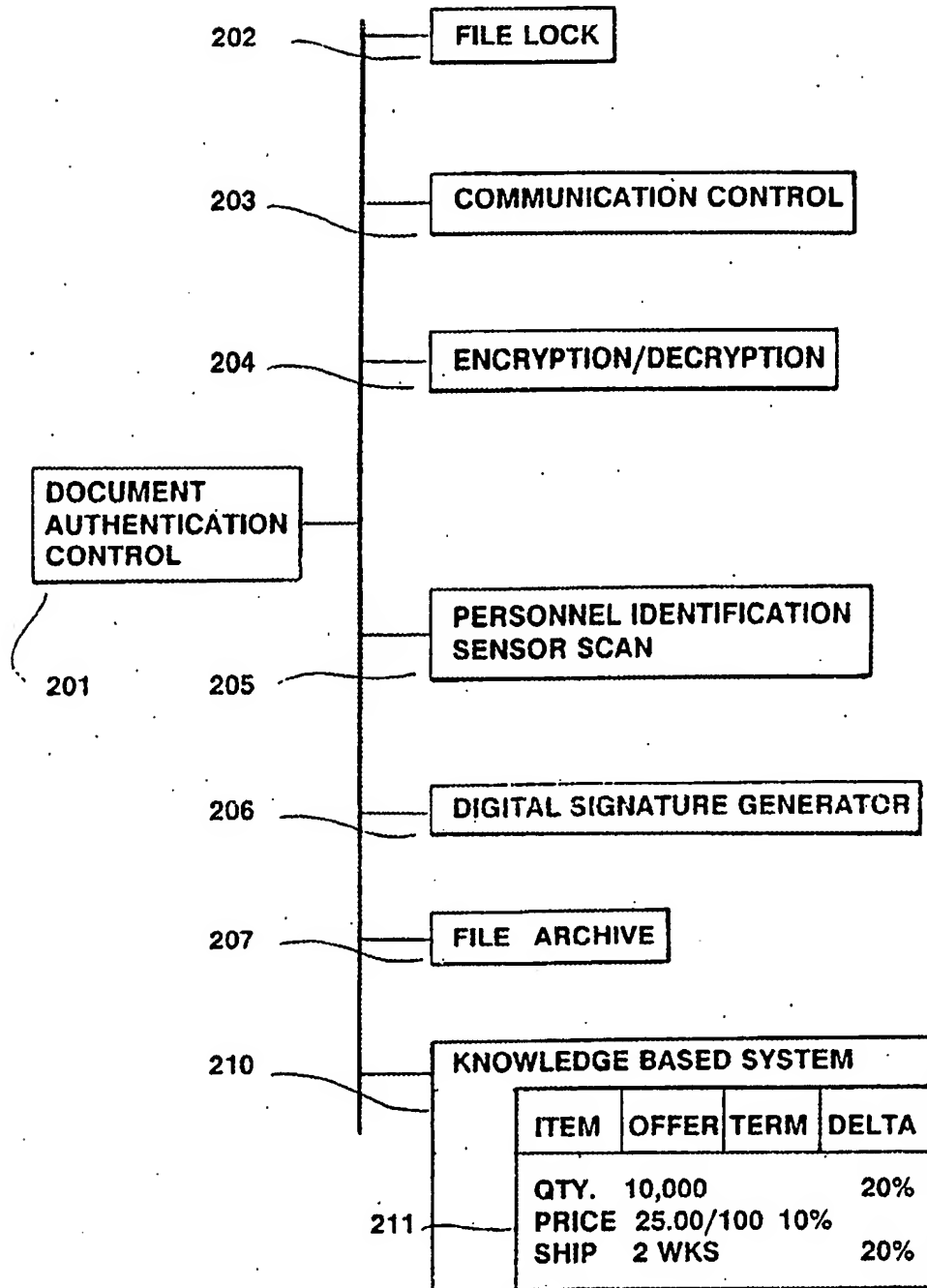


FIG. 2

3/6

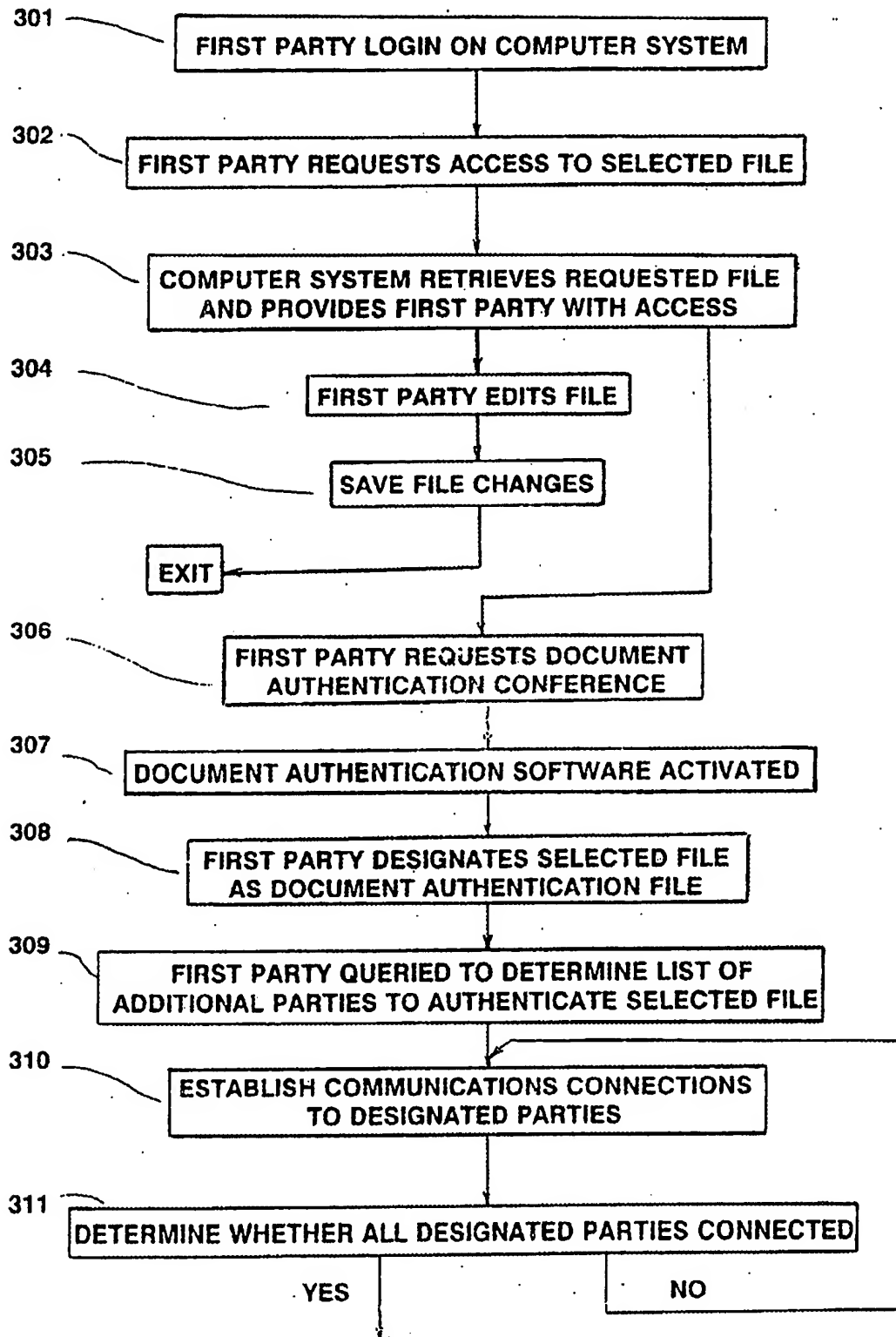


FIG 3

4/6

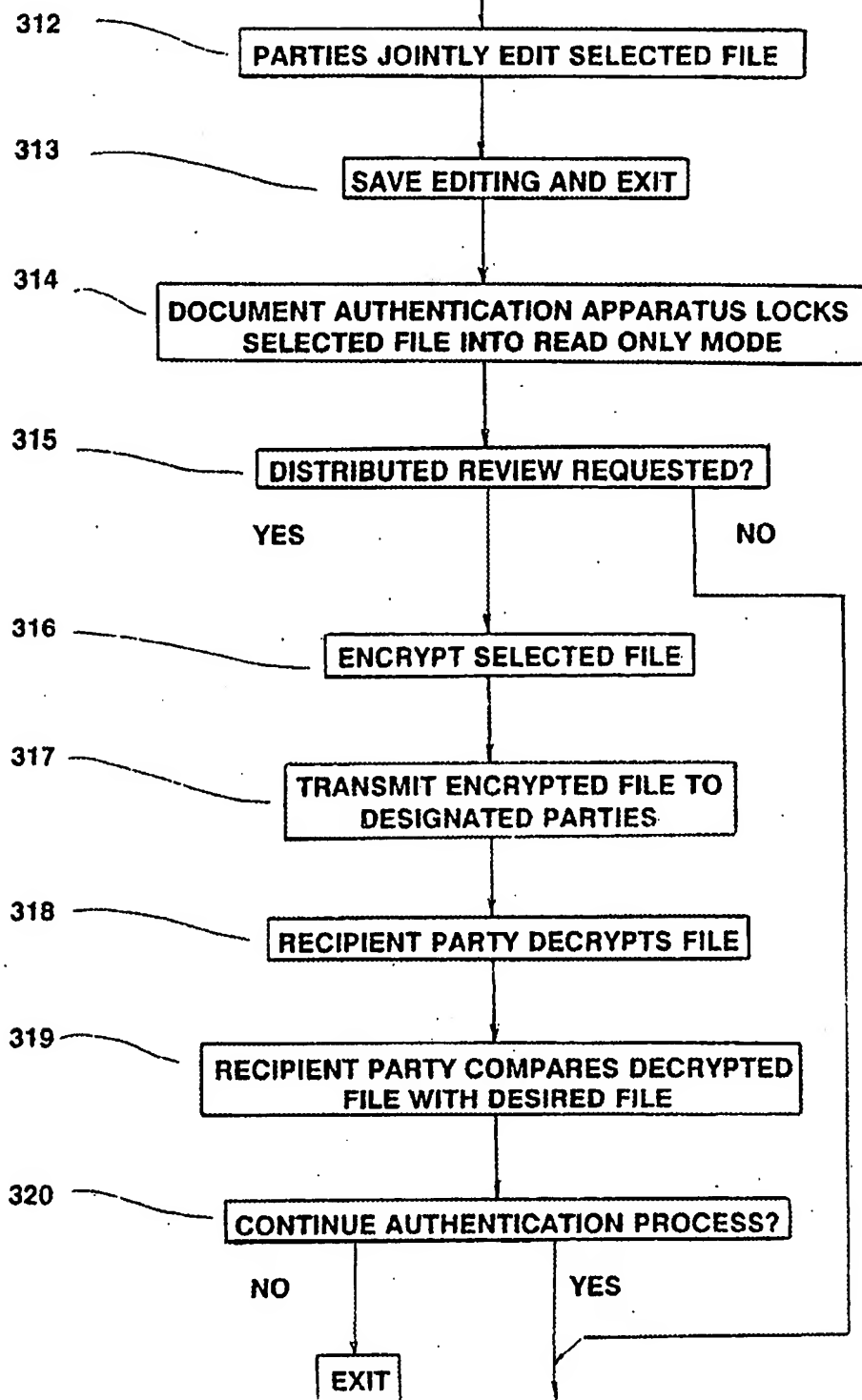


FIG 4

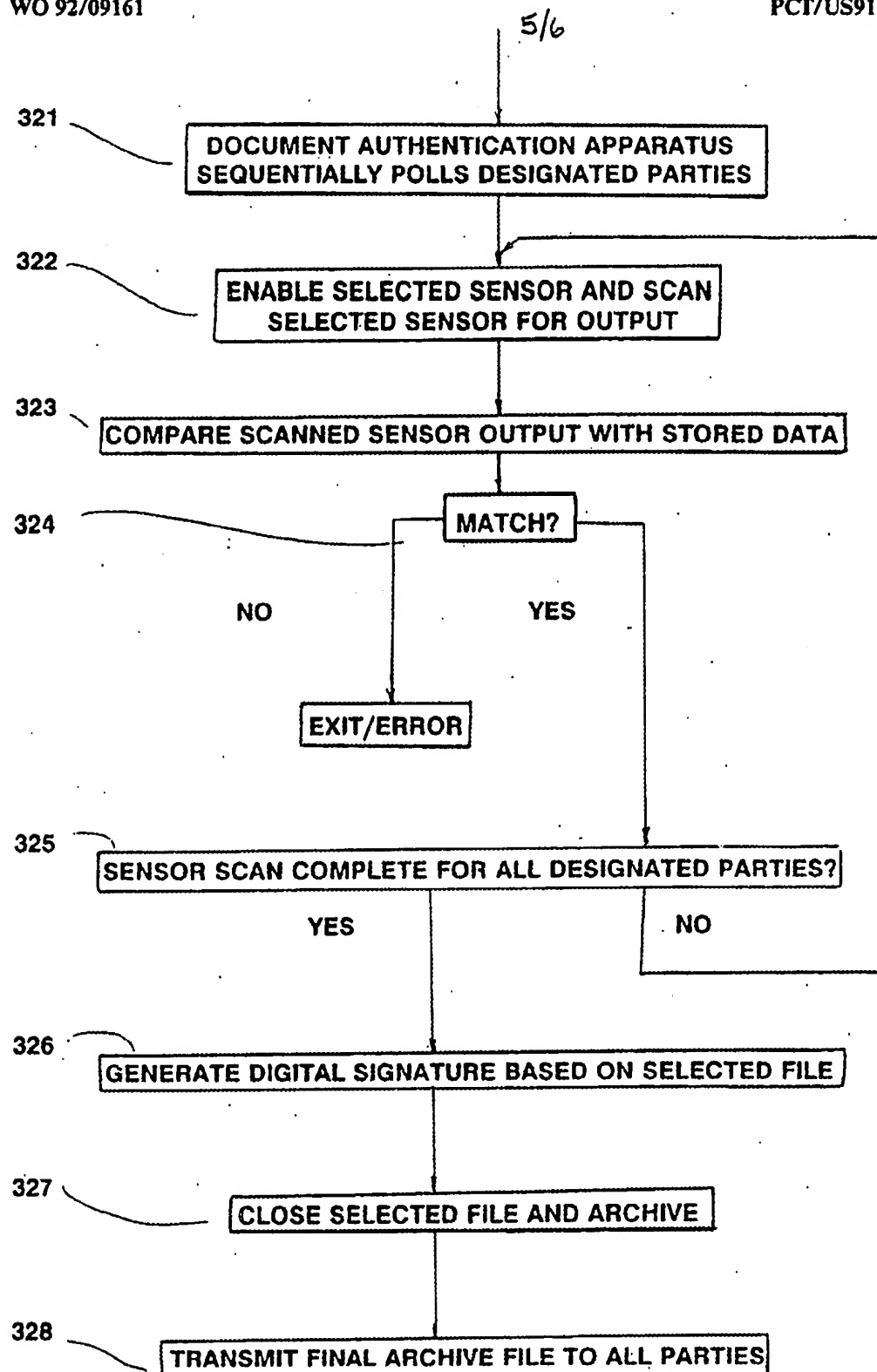


FIG 5

6/6

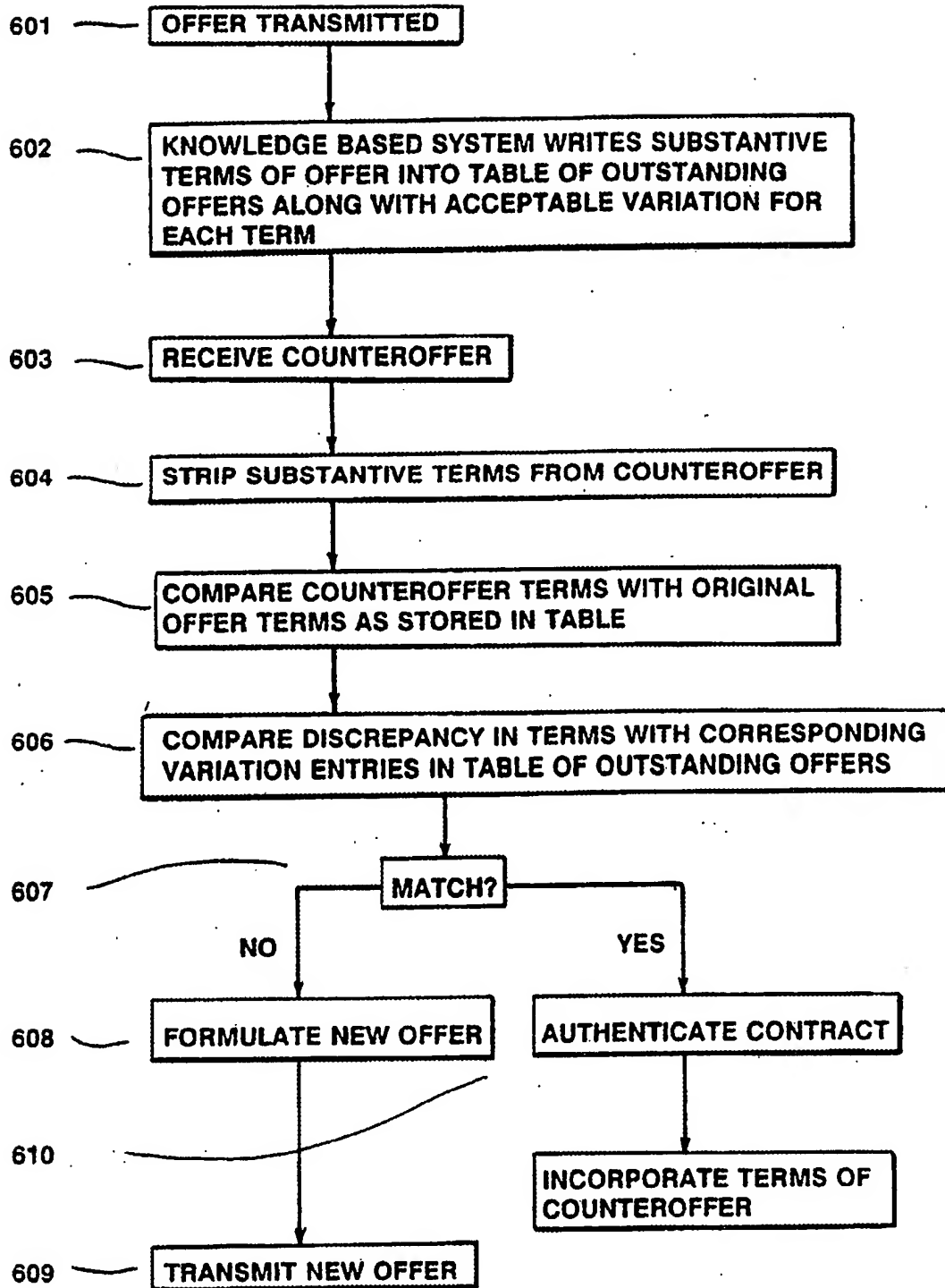


FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No PCT/US91/08545

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all) ¹		
According to International Patent Classification (IPC) or to both National Classification and IPC IPC (5): H04L 9/32 U.S. Cl.: 380/25		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁴		
Classification System	Classification Symbols	
U.S.	340/825.31, 825.34 380/23, 24, 25, 49, 50 235/379, 380, 381, 382	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁵		
III. DOCUMENTS CONSIDERED TO BE RELEVANT ¹⁴		
Category ⁶	Citation of Document, ¹⁶ with indication, where appropriate, of the relevant passages ¹⁷	Relevant to Claim No. ¹⁸
A	US, A, 4,453,074 (WEINSTEIN) 05 June 1984	1-20
A	US, A, 4,568,936 (GOLDMAN) 04 February 1986	1-20
A	US, A, 4,633,036 (HELLMAN ET AL.) 30 December 1986	1-20
A	US, A, 4,807,287 (TUCKER ET AL.) 21 February 1989	1-20
A	US, A, 4,893,338 (PASTOR) 09 January 1990	1-20
A	US, A, 4,893,340 (LUBARSKY ET AL.) 09 January 1990	1-20
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>¹⁵ Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="width: 48%;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"d" document member of the same patent family</p> </div> </div>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search ¹⁹	Date of Mailing of this International Search Report ²⁰	
13 January 1992	04 FEB 1992	
International Searching Authority ¹	Signature of Authorized Officer ²⁰	
ISA/US	In Bernarr Earl Gregory <i>Bernarr Earl Gregory</i> NGSTEN NGOC-HO INTERNATIONAL DIVISION	